Cyber cold war

(264)—Scada, Stuxnet, token crittografici e Mutual Assured Destruction. La sicurezza non interessa a nessuno: sottili equilibri di…

Cyber cold war

(264)—Scada, Stuxnet, token crittografici e Mutual Assured Destruction. La sicurezza non interessa a nessuno: sottili equilibri di potere sorreggono un sistema pieno di buchi.

20 novembre 2012—Come dice Wikipedia, in informatica, l'acronimo SCADA (dall'inglese "Supervisory Control And Data Acquisition", cioè "controllo di supervisione e acquisizione dati") indica un sistema informatico distribuito per il monitoraggio elettronico di sistemi fisici.
In pratica, specialmente quando si discute di sicurezza e guerra cibernetica, si intende quella classe di componenti hardware che controllano sistemi importanti come distribuzione elettrica, acquedotti, raffinerie, centrali nucleari: la cosa è importante perché i componenti di questi sistemi comunicano tra loro in reti WAN di tipo TCP o 3G, quando non addirittura attraverso Internet. Ormai da anni si discute dell'indifendibilità di questi sistemi di fronte ad attaccanti informatici preparati e decisi.

Stuxnet è un nome che non ha bisogno di spiegazione (se ne avesse, cliccate qui): un malware che ha soppiantato l'Internet Worm di Morris sui libri di storia della Rete, e che rappresenta la prima arma informatica utilizzata con successo a fini tanto ostili quanto precisi su un bersaglio ben identificato (per la cronaca, gli impianti di arricchimento di esafluoruro di uranio in Iran). L'arma è ancora attiva, come ben testimonia questo articolo.

I token crittografici RSA sono gadget da portachiavi che visualizzano un PIN di 6 cifre che cambia continuamente, e che vengono usati come one-time-password da banche ed altri fornitori di servizi per autenticare gli utenti; molte aziende li usano per identificare gli utenti che da remoto vogliono collegarsi alla rete aziendale.

Nel 2011 è stato confermato che la rete interna di un importantissimo costruttore di armamenti americano, Lockheed Martin, era stata violata superando un sistema di accesso protetto da questi token. Il costruttore dei token ha poi confermato, in grande ritardo e a malincuore, che gli erano stati sottratte le informazioni necessarie a violare la sicurezza di tutti i token prodotti fino ad allora. In pratica, era stato sottratto un file contenente i "semi" crittografici dei token prodotti, associati con le relative matricole di fabbrica. Questo file non avrebbe nemmeno dovuto esistere, ma approfondire il discorso richiederebbe un articolo a parte. Il costruttore però non è stato sommerso dalle cause e fatto fallire, anzi pare essere stato lasciato del tutto indenne. Come mai?MAD (Mutual Assured Destruction—distruzione reciproca assicurata) è la strategia che

USA e URSS hanno usato per decenni al fine di tenere in equilibrio il mondo prevenendo una guerra termonucleare globale. Il concetto, che ha funzionato per decenni era “Se tu mi attacchi con dei missili nucleari, io riesco comunque a lanciare abbastanza missili nucleari da distruggerti”. Che fosse perché il lancio veniva avvistato ed i missili di rappresaglia potessero partire prima dell’arrivo di quelli attaccanti, o perché le basi missilistiche superstiti potevano lanciare abbastanza missili di rappresaglia, poco importava.Ah, val la pena di notare che se la cosa non avesse funzionato, ora non saremmo qui a preoccuparci di terrorismi e riscaldamento globale.

Quale filo logico, anzi paranoico, tiene insieme questi quattro fatti?

E’ piuttosto semplice. Oggi si fa un gran parlare di sicurezza informatica, di guerra cibernetica. Si creano, all’estero e persino in Italia, enti ed organizzazioni ben finanziate che si occupano di studio e difesa (ed offesa) in questo campo. Sembra che tutti siano coscienziosi e stiano correndo ai ripari.Ma come gli addetti ai lavori ed anche i semplici interessati vedono ogni giorno, niente o quasi niente sta cambiando. I sistemi SCADA, ma anche i sistemi informatici, sono poco sicuri come in passato. Anzi, poiché nel frattempo stanno evolvendo e complicandosi, sono sempre meno sicuri.Le uniche attività di aumento della sicurezza sono il turare le falle più clamorose, come le password lasciate di default o peggio ancora cablate nel software o nel firmware.Persino attacchi informatici che portano alla compromissione totale e perpetua di un sistema di sicurezza come quello dei token crittografici RSA SecurID non provocano una sostituzione del sistema: conosco molte situazioni in cui i token incriminati e notoriamente compromessi continuano ad essere utilizzati, e non parlo della cassa mutua di un paesino della Bassa Padana, ma di multinazionali globali.Cosa si può concludere? Beh, nel caso generale, ma sopratutto riguardo ai sistemi SCADA, che mettere in sicurezza le cose non interessa a nessuno.

Una giustificazione aziendale è che i costi di adeguamento dei sistemi sono insostenibili e graverebbero sugli utenti, una più *andreottiana* è uguale nella prima parte, ma finisce dicendo che le spese graverebbero sui profitti dell’azienda.

Il discorso paranoico diventa interessante se portato a livello di guerra cibernetica. Poiché almeno Stati Uniti, Cina e Russia son ormai da anni dotate di organizzazioni dedicate all’argomento, e visto che la cronaca di Stuxnet ne fornisce una conferma clamorosa, perché le suddette superpotenze non si impegnano in una vera e propria corsa alla messa in sicurezza degli impianti dotati di controlli SCADA?Beh, oltre ai soldi una spiegazione che giustifica la staticità di questa situazione e la mancanza di azioni ostili può essere un equilibrio del terrore anche in questo campo, un accordo più o meno tacito e sicuramente non pubblico a non premere il bottone per primi per evitare una reazione altrettanto distruttiva.

E magari anche per poter spendere i soldi disponibili non per rendere gli impianti SCADA più sicuri, ma in importanti azioni di guerra ^h^h^h^h^h^h^h^h missioni di pace.

E **giustifica anche il fatto che un grande player della sicurezza informatica non venga punito quando commette un errore titanico**. Insomma, su sicurezza, guerra cibernetica e SCADA forse non si gioca a guardie contro ladri, ma si persegue un bilancio di potere.

Originally published at punto-informatico.it.

By Marco A. L. Calamari on March 19, 2021.

Canonical link

Exported from Medium on January 2, 2024.